Chapter 2: Algebraic structures part 1

Hamza Moufek

Algebra 1

November 2024

المدرسة الوطنية العليا في الأمن السيبراني
NATIONAL SCHOOL OF CYBERSECURITY

Outlines of this talk

- Binary operations
- Groups
- Subgroups
- Group homomorphisms

Definition

Definition

A binary operation on a set S is a function

$$\begin{array}{cccccc} * & : & S \times S & \to & S \\ & & (a,b) & \mapsto & *(a,b) \end{array}$$

For convenience we write $a * b$ instead of $*(a,b)$.The set S is said closed under the operation $*$. We call the data of a set S together with a binary operation $*$,written $(S;*)$, magma.
Binary operations are usually denoted by other symbols (for example, $+$ or $\times$ for numbers) but, for the moment, we use the generic notation $a * b$.

Figure: 1

Example 1

- Let $S = \mathbb{R}$ and $*$ be $+$. For $a, b \in \mathbb{R}$, $a * b = a + b$, addition (note that $a + b \in \mathbb{R}$). This is a binary operation.
- Let $S = \mathbb{Z}$ and $*$ be $\times$. For $a, b \in \mathbb{Z}$, $a * b = ab$, multiplication (note that $ab \in \mathbb{Z}$). This is a binary operation.
- Let $S = \mathbb{Z}$ and $a * b = \max\{a, b\}$, the largest of a and b. This is a binary operation.
- Let $S = \mathbb{Q}$ and define $*$ by $a * b = a$. This is a binary operation.
- Let $S = \mathbb{Z}$ and $a * b = \frac{a}{b}$. This is not a binary operation,as it's not defined when $b = 0$, and also $\frac{a}{b}$ need not be in $\mathbb{Z}$.
- Let $S = \{f : A \longrightarrow A\}$, with $*$ composition of functions and A non empty set. This is a binary operation.
- Let X be a set. On $\mathcal{P}(X)$, the union of

$$\mathcal{P}(X)^2 \to \mathcal{P}(X)$$
$$(A, B) \mapsto A \cup B$$

is a binary operation. The same,for the intersection $A \cap B$ and symmetric difference $A \bigtriangleup B$.

Example 2

Example 2

A binary operation $\triangle$ is defined on the set $\mathbb{R}$of real numbers by

$$a \triangle b = \frac{2a-b}{a^2+2}, \text{where} \quad a, b \in \mathbb{R}$$

Evaluate: $(a) \quad 2 \triangle 3$, $(b) \quad 3 \triangle 2$.

Solution

$(a) \quad 2 \triangle 3 = \frac{2.2-3}{2^2+2} = \frac{1}{6}, \qquad (b) \quad 3 \triangle 2 = \frac{2.3-2}{3^2+2} = \frac{4}{11}.$

Example 3

Example 3

The operation $\overline{+}$ is defined on the set $S=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$ by Table below

$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

RemarkThese table (Cayley table for the magma $(\mathbb{Z}/5\mathbb{Z},\overline{+})$)defines the operation $\overline{+}$ on the set S. The set S is closed with respect to $\overline{+}$ since when any two elements of S are combined, the result is always an element of S. That is,

$$\forall x,y\in S\Rightarrow x\overline{+}y\in S.$$

for example $\overline{3}\overline{+}\overline{2}=\overline{0}$ and $(\overline{3}\overline{+}\overline{1})\overline{+}\overline{2}=\overline{1}$ an other example with operation table:

Commutative operations

Definition

A binary operation $*$ defined on a set E is said to be commutative if $a * b = b * a$, for all $a, b \in E$.

Remark Addition $(+)$ and multiplication $(\times)$ are both commutative since for all $a, b \in \mathbb{R}$, $a + b = b + a$ and $a \times b = b \times a$.

The union $(\cup)$ and the intersection $(\cap)$ are both commutative since for any two sets A and B,$A \cup B = B \cup A$ and $A \cap B = B \cap A$.

EXAMPLE 1

The operation $*$ is defined on the set of real numbers $\mathbb{R}$ by $a * b = a + b + 2ab$. Show that $*$ is commutative.

$$
\begin{aligned}
a * b &= a + b + ab......(1)\\
b * a &= b + a + ba\\
&= a + b + ab......(2)\ [\textbf{since } a + b = b + a \textbf{ and } ab = ba \textbf{ for all } a, b \in \mathbb{R}\ ]
\end{aligned}
$$

Comparing (1) and (2) it follows that $a * b = b * a$ for all $a, b \in \mathbb{R}$. Hence the operation $*$ is commutative.

EXAMPLE 2

The operation $\bigtriangledown$ is defined on the set $\mathbb{R}$ of real numbers by $x \bigtriangledown y = x - y + 3xy$.

$$
\begin{aligned}
x \bigtriangledown y = x - y + 3xy.............(1)\\
y \bigtriangledown x = y - x + 3yx.............(2)
\end{aligned}
$$

Since subtraction is not commutative it follows that $x - y \neq y - x$ and therefore $x \bigtriangledown y \neq y \bigtriangledown x$. Hence the operation $\bigtriangledown$ is not commutative.

ASSOCIATIVITY

Definition

A binary operation $*$ defined on a closed set E is said to be associative if for every $a, b, c, \in E, (a * b) * c = a * (b * c) = a * b * c$.

Example 1

Show that the operation $*$ defined over the set of real numbers $\mathbb{R}$ is associative, where $a * b = a + b + ab$.

$$\begin{aligned}
(a * b) * c &= (a + b + ab) * c \\
&= (a + b + ab) + c + (a + b + ab)c \\
&= a + b + c + ab + ac + bc + abc............(1) \\
a * (b * c) &= a * (b + c + bc) \\
&= a + (b + c + bc) + a(b + c + bc) \\
&= a + b + c + bc + ab + ac + abc...........(2)
\end{aligned}$$

From (1) and (2), $(a * b) * c = a * (b * c)$ for all $a, b, c \in \mathbb{R}$. Hence the operation $*$ is associative

exercise The operation defined on the set $\mathbb{R}$ of real numbers by $a \triangle b = ab + a$. Determine whether or not the operation $\triangle$ is associative.

Definition

Let $*$and $\triangle$ be two binary operations both defined on the closed set E . We say the operation $*$ is distributive over $\triangle$ if for all $a, b, c \in E, a * (b \triangle c) = (a * b) \triangle (a * c)$ and $(b \triangle c) * a = (b * a) \triangle (c * a)$

Example

- For example, multiplication $(\times)$ is distributive over addition $(+)$ since for all $a, b, c \in \mathbb{R}, a \times (b + c) = (a \times b) + (a \times c)$ and $(b + c) \times a = (b \times a) + (c \times a)$ written as $a(b + c) = ab + ac$.
- In the set $\mathcal{P}(X)$ of parts of a set X, the union is distributive with respect to the intersection and the intersection is distributive with respect to the union

$$\forall A, B, C \in \mathcal{P}(X) \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$\forall A, B, C \in \mathcal{P}(X) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

.

Identity or neutral elements

Definition

Let $*$ be a binary operation on a non empty set A. An element e is called an identity element with respect to $*$ if

$$e * x = x = x * e$$

for all $x \in A$.

Examples

- 1 is an identity element for multiplication on the integers.
- 0 is an identity element for addition on the integers.
- If $*$ is defined on $\mathbb{Z}$ by $x * y = x + y + 1$ Then -1 is the identity.
- The operation $*$ defined on $\mathbb{Z}$ by $x * y = 1 + xy$ has no identity element.

Identity or neutral elements

Exercise 1

The operation $*$ is defined over the set $\mathbb{R}$ of real numbers by $a * b = a + b + 2ab$. Find the identity element under the operation $*$.

Solution Let $e \in \mathbb{R}$ be the identity element under the operation $*$. It then follows that for every element $a \in \mathbb{R}$, $a * e = e * a = a$. Solving for e we have

$$\begin{aligned} a * e = a &\Rightarrow a + e + 2ae = a \\ &\Rightarrow e(1 + 2a) = 0 \\ &\Rightarrow e = 0 \end{aligned}$$

Hence the identity element under $*$ is 0.

Inverse Element

Definition

Let be a set equipped with a binary operation $*$ that admits an identity element e.We say that an element $x \in G$ is invertible if there exists an element $y \in G$ such that:

$$x * y = y * x = e$$

We say then that $y$is the inverse of x.

Remark

- When the binary operation is denoted additively:$+$(resp. multiplicatively: $\times$), the identity element will be denoted by 0(resp. 1)
- the inverse of x will be denoted by $-x$ (resp.x^{-1}).

Example

- Consider the operation of addition on the integers. For any integer a, the inverse of a with respect to addition is $-a$.
- Consider the operation of multiplication on $\mathbb{Z}$. The invertible elements are 1 and -1.
- In $\mathbb{R}$, each element a has an inverse for addition which is its opposite $-a$. But a has only an inverse for multiplication if it is non-zero; its inverse is then the inverse $1/a$ of a.
- In $\mathcal{F}(X, X)$, an element f has an inverse (for the composition $\circ$) if and only if f is bijective and then its inverse is the reciprocal map f^{-1}.

Inverse Element

Exercise 2

The operation $*$ is defined over the set $\mathbb{R}$ of real numbers by

$$a * b = a + b + 2ab, \textbf{ for all} a, b \in \mathbb{R}.$$

Find the inverse under $*$ of a general element $a \in \mathbb{R}$ and state which element has no inverse. Determine the inverses of 2 and 3.

For $a \in \mathbb{R}$, let $a^{-1} \in \mathbb{R}$ be the inverse. From Exercise 1 , the identity element is $e = 0$ so :

$$\begin{aligned} a * a^{-1} = a^{-1} * a = e = 0 \\ a + a^{-1} + 2aa^{-1} = 0 \\ a^{-1} + 2aa^{-1} = -a \\ a^{-1}(1 + 2a) = -a \\ a^{-1} = \frac{-a}{1 + 2a} \end{aligned}$$

The inverse expression a^{-1} becomes undefined when the denominator is zero. so:

$$a^{-1} \textbf{is not defined} \Leftrightarrow 1 + 2a = 0$$

Hence $\frac{-1}{2}$ has no inverse. The inverse of 2 is $\frac{-2}{5}$ and the inverse of 3 is $\frac{-3}{7}$.

Definition

Definition of Group

Let G be a non-empty set and $*$ a binary operation on G. We call $(G, *)$ a group if the following hold:

- The operation $*$is associative.That is, for all $a, b, c \in G$ we have that $(a * b) * c = a * (b * c)$.
- The operation $*$admits an identity element $e \in G$.That is, there is an $e \in G$ so that for all $a \in G$ we have that $e * a = a * e = a$.
- Every element of G is invertible.That is, for every $a \in G$ there is an $\tilde{a} \in G$ so that $a * \tilde{a} = \tilde{a} * a = e$.

Moreover, a group is called commutative or Abelian group iff $*$ is commutative.

Examples

- $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ and $(\mathbb{C},+)$ are commutative groups.
- $(\mathbb{N},+)\quad and(\mathbb{Z},\times)$ are not groups.
- Let G be the set of bijective functions from $A\longrightarrow A$,and let $\circ$ be the operation of composition of functions. Then$(G,\circ)$is a non commutative group. With neutral element:id_A, inverse element of f **is** f^{-1}
- Let $=\mathbb{Z}/5\,\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$ be the set of integers modulo 5 .Set

  $$\forall\overline{x},\overline{y},\overline{x}\overline{+}\overline{y}=\overline{x+y}$$

  This operation is well defined,and $(G,\overline{+})$ is an abelian group.
- Let G be the set $\{1,-1\}$. Then it forms an abelian group under multiplication.
- The subset $\{1,-1,i,-i\}$ of the complex numbers is a group under complex multiplication. Note that -1 is its own inverse, where as the inverse of i is $-i$, and vice versa.

THEOREME

Let $(G, *)$ be a group. Then we have:

- The identity element is unique.
- For all $a, b, x \in G$,we have the cancellation laws

$$a * x = b * x \Rightarrow a = b,$$

  and

$$x * a = x * b \Rightarrow a = b.$$

- For all $x \in$,the inverse of x is unique.
- For all $x \in$,the inverse of x^{-1} is x.
- For all $x, y \in, (x * y)^{-1} = y^{-1} * x^{-1}$.

Definition and Properties

Let G be a group with binary operation $*$. For any $a \in G$ we define *nonnegative integral exponents* by

$$a^0 = e, \qquad a^1 = a, \qquad a^{n+1} = a^n * a \quad n > 0.$$

Negative integral exponents are defined by

$$a^{-n} = (a^{-1})^n \qquad n > 0.$$

With

$$a^n = \underbrace{a * a * a * .... * a}_{\textbf{n times}}$$

Laws of Exponents

$1) x^n \cdot x^{-n} = e, \qquad 2) x^m \cdot x^n = x^{m+n} \qquad 3) (x^m)^n = x^{mn}$

and If G is abelian then

$4) (xy)^n = x^n y^n.$

Definition

Definition 1

If a subset **H** of a group **G** is itself a group under the operation of **G**, we say that **H** is a subgroup of **G**

Remark If $(G, *)$ is a group and $H \subseteq G$ with $(H, *)$ is also a group , then H is a subgroup of a group G

Definition 2

Let $(G, *)$ be a group. A subgroup of G is a subset $H \subseteq G$ that satisfies the following:

- $e_G \in H$
- $\forall x, y \in H, x * y \in H.$
- $\forall x \in H, x^{-1} \in H.$

Remark A subgroup is a group under the induced binary operation, with the same identity element.

Characterization of subgroups and Example

Theoreme

A non void subset H of a group $(G, *)$ is a subgroup of G iff :

$$\forall (a, b) \in H^2, a * b^{-1} \in H.$$

Examples

- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are subgroups of $(\mathbb{C}, +)$
- $(]0, +\infty[\,, \times)$ is a subgroup of $(\mathbb{R}^*, \times)$.

Exercise 1

Let G group. Let

$$Z(G) = \{x \in G \mid x * g = g, \textbf{for all} \quad g \in G\}$$

Show that $Z(G)$ is a subgroup of G.

Exercise 2

Show that intersection of two subgroups of a group G is a subgroup of G.

Exercise
show that the union of two subgroups is not a subgroup
proof
Let

$$H_2 = \{2n | n \in \mathbb{Z}\}$$

and

$$H_3 = \{3n | n \in \mathbb{Z}\}$$

Wher $(\mathbb{Z}, +)$ is the group of integers . H_2 and H_3 will be subgroups of $\mathbb{Z}$. Indeed

$$2n - 2m = 2(n - m) \in H_2$$

and

$$3n - 3m = 3(n - m) \in H_3$$

Now $H_2 \cup H_3$ is not a subgroup as $2, 3 \in H_2 \cup H_3$ but

$$2 - 3 \notin H_2 \cup H_3$$

THE union of two subgroups is a subgroup iff one of them is contained in the other

Definition

Definition

Let $(G, *)$ and $(G', \diamond)$ be two groups. A map $f : G \to G'$ is said to be a group homomorphism if

$$\forall x, x' \in G \ \phi(x * x') = \phi(x) \diamond \phi(x')$$

Then, ϕ is group homomorphism .

Remark

Not every function from one group to another is a homomorphism! The condition $\phi(a * b) = \phi(a) \diamond \phi(b)$ means that the map ϕ preserves the structure of G.

Examples

Example 1

Let G be the group $(\mathbb{R}, +)$ and G' be the group $(\mathbb{R}_+^*, \times)$. The map $f : \mathbb{R} \to \mathbb{R}_+^*$ defined by $f(x) = e^x$ is an homomorphism.
Indeed, we have

$$\forall x, y \in \mathbb{R}, f(x+y) = e^{x+y} = e^x \times e^y = f(x) \times f(y).$$

Example 2

Consider the function

$$\begin{array}{cccc} \varphi & : & (\mathbb{Z}, +) & \to & (\mathbb{Z}/5\,\mathbb{Z}, \overline{+}) \\ & & x & \mapsto & \overline{x} \end{array}$$

for all $(a, b) \in \mathbb{Z}$,we have $\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a)\overline{+}\varphi(b)$

Types of homomorphisms

- A homomorphism that is both injective and surjective is an isomorphism.
- Two groups are isomorphic if there exists an isomorphism between them .
- A homomorphism from a group to itself is called an endomorphism.
- An automorphism is an isomorphism from a group to itself .

Two basic properties of homomorphisms

Proposition

Let $\phi : G \longrightarrow H$ be a homomorphism. Denote the identity of G by 1_G , and the identity of H by 1_H.

- $\phi(1_G) = 1_H$ "ϕ sends the identity to the identity"
- $\phi(g^{-1}) = \phi(g)^{-1}$ "ϕ sends inverses to inverses "

Example

Let G be the group $(\mathbb{R}, +)$ and G' be the group $(\mathbb{R}_+^*, \times)$. The map $f : \mathbb{R} \mapsto \mathbb{R}_+^*$ defined by $f(x) = e^x$. We have $f(0) = 1$. The identity element of $(\mathbb{R}, +)$ has as its image the identity element of $(\mathbb{R}_+^*, \times)$. For $x \in \mathbb{R}$ its inverse in $(\mathbb{R}, +)$ is here its opposite $-x$, Then $f(-x) = e^{-x} = \frac{1}{e^x} = \frac{1}{f(x)}$ is the inverse of $f(x)$ in $(\mathbb{R}_+^*, \times)$.

Proposition

- Let $\varphi : G \to G'$ and $\phi : G' \to G"$ be two groups homomorphisms. The $\phi \circ \varphi : G \to G"$ is a group homomorphism.
- If $\varphi : G \to G'$ is a bijective homomorphism, then $\varphi^{-1} : G' \to G$ is also a group homomorphism.

Group Homomorphism

Definition

Given $\varphi : G \to G'$ a homomorphism of groups, we define the **kernel** of φ to be:

$$Ker(\varphi) = \{x \in G | \varphi(x) = e_{G'}\}$$

We define the image of φ to be:

$$Im(\varphi) = \{y \in G' | \exists x \in G \text{ such that } \varphi(x) = y\}$$

Proposition

Let $\varphi : G \to G'$ be a group homomorphism. Then we have :

- The **kernel** of φ,ker(f) is a subgroup of G.
- The **image** of φ,$Im(f)$ is a subgroup of G'.
- The homomorphism φ is injective if, and only if, ker$(\varphi) = \{e_G\}$.
- φ is surjective if, and only if, $Im(\varphi) = G'$.